



UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

09/429,624 10/29/99 YUNG

M 10624.0015

EXAMINER

WM31/0629

SONG, H

STUART T F HUANG  
STEPTOE & JOHNSON LLP  
1330 CONNECTICUT AVENUE NW  
WASHINGTON DC 20036-1795

ART UNIT

PAPER NUMBER

2131

DATE MAILED:

06/29/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

# Office Action Summary

Application No.  
**09/429,624**

Applicant,  
**YUNG**

Examiner  
**Ho S. Song**

Art Unit  
**2131**



-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on Apr 4, 2001
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above, claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claims \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are objected to by the Examiner.
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).
- a) ☐ All b) ☐ Some\* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \*See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

## Attachment(s)

- 15) ☐ Notice of References Cited (PTO-892) 18) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 19) ☐ Notice of Informal Patent Application (PTO-152)
- 17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). \_\_\_\_\_ 20) ☐ Other:

Art Unit: 2131

### **DETAILED ACTION**

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

#### ***Docketing***

2. Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record, using the information supplied in the final section of the office action.

#### ***Claim Rejections - 35 USC § 102***

4. The previous action is incorporated by reference in its entirety. Particularly, the specific indication of various claim elements which will not be reiterated in this action. The statutory basis for each rejection is repeated below:

a. Claims 1-10 are rejected under 35 U.S.C. 102(a) as being anticipated by Gennaro et al.(hereinafter, "Gennaro") in *Robust Threshold DSS Signatures*.

b. Claims 1-4 and 9-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Brickell et al.(hereinafter, "Brickell")(US 5,867,578).

#### ***Response to Amendment***

5. The rejections based on Gennaro(Robust Threshold DSS Signatures) and Brickell(US 5,867,578) of the previous action are maintained.

Art Unit: 2131

6. Claims 1-11 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-11 of U.S Patent No.6,035,041 are withdrawn in view of Applicant's arguments filed 4/4/01.

7. Mark-up copy of an Amendment is missing. Claim 1 is not entered. Examiner contacted the Applicant's representative(Mr. Huang) on 4/26 to provide a mark-up copy of an Amendment.

8. Applicant has added claims 12-22. The grounds of rejection are presented below.

9. Applicant's arguments filed 4/4/01 have been fully considered but they are not persuasive.

Applicant argues that Gennaro et al. does not disclose a step of generating random values using the shared values.

Response: Gennaro discloses calculation of random number using the shared values in (page 365). k being random secret value using Joint Shamir RSS.

Applicant argues that Brickell does not disclose generating random values from shared values.

Response: Brickell discloses generating random values from shared values are disclosed in (col.9, lines 10-65).

### ***Claim Rejections - 35 USC § 102***

10. Claims 12-22 are rejected under 35 U.S.C 102(e) as being anticipated by Brickell et al.(hereinafter, "Brickell")(US 5,867,578).

As per claim 12, Brickell discloses computing shared values, generating random values using shared values and at each plurality of the distributed electronic devices , generating a partial result

Art Unit: 2131

for the cryptographic computation using a shared of the cryptographic values and at least one of random values and computation of a final result using partial result in (fig.1, col.9, lines 10-65).

In claims 13-16, Brickell discloses shared value is shared among a subset of the distributed electronic devices in (fig.1,col.14, lines 29-67).

In claims 17-22, Brickell discloses each of a plurality of shared values is shared among a pair of the distributed electronic devices in (col.10, lines 41-51).

### ***Conclusion***

11 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2131

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ho S. Song whose telephone number is 703-305-0042.

The examiner can normally be reached on Tues-Fri between the hours of 6:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703-305-9711. The fax number for the organization is 703-305-0040.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305 3900.

*Ho Song*

*Gail Hayes*

**GAIL HAYES**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**